

AHEAD OF WHAT'S NEXT.

IT Security

Final Report

July 2011

Prepared for:



Introduction

Methodology

Who

N=200 total interviews were conducted among a targeted online ITDM panel.

Respondents were qualified as:

- IT decision makers/influencers
- Involved in making decisions about IT security
- Working in an enterprise sized company with at least 1000 employees

Data were weighted by company size, giving relatively greater weight to larger companies.

When

Interviews were conducted April 19 – May 3, 2011

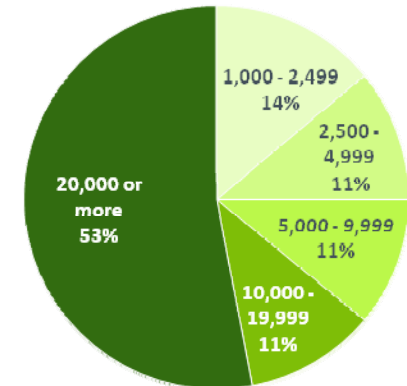
How

Via self-administered online survey

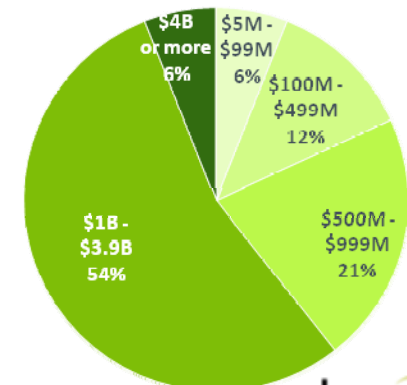
Significance Notations

Significance testing was conducting at the 90% confidence level. When comparisons among three or more groups have been made, letters (A/B/C/D) are used to indicate a value that is significantly greater than the group referenced. For comparisons between two groups arrows (↑↓) indicate a number is significantly higher/lower than the other group.

Company Size (# employees)



Company's Gross Total Revenue



Executive Summary

Executive Summary

Today's IT Security Landscape

Today's landscape for the enterprise ITDM is one where information security breaches are very common.

- Approximately eight in ten have experienced the following in the past two years: system glitches/errors (80%), unintentional mistakes/misuse (77%), malware (76%), lost/stolen equipment (75%).
- Another seven in ten have experienced external data theft (74%) and insider data theft (72%).

These breaches represent cause for concern, with nearly all ITDMs expressing they are at least “somewhat concerned” and four in ten indicating they are “very concerned”.

That said, there are signs of optimism.

- Nearly all agree today's IT security solutions are better than those 5 years ago. Four in ten (44%) believe they are “much better”.
- Most are confident in their organization's IT security solution capabilities. They have the highest level of confidence in their ability to “monitor workers access to organization's various resources at all times” and least confident in their ability to “successfully monitor and security consumer devices, such as a smart phone.”

Key challenges include:

- “Lack of time to monitor vast amounts of data” (64%).
- “Unable to manage security in cloud” (55%) or “virtualized” (54%) environments.

Executive Summary

IT Security Budgets and Solutions

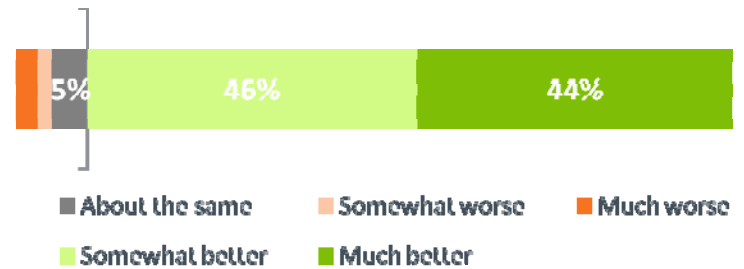
Perhaps as a result of the proliferation of security breaches, as well as a strengthening economy, nearly eight in ten (77%) indicate IT security budgets are higher this year compared to last.

On average, over one-half (59%) of enterprise IT budget is allocated towards security.

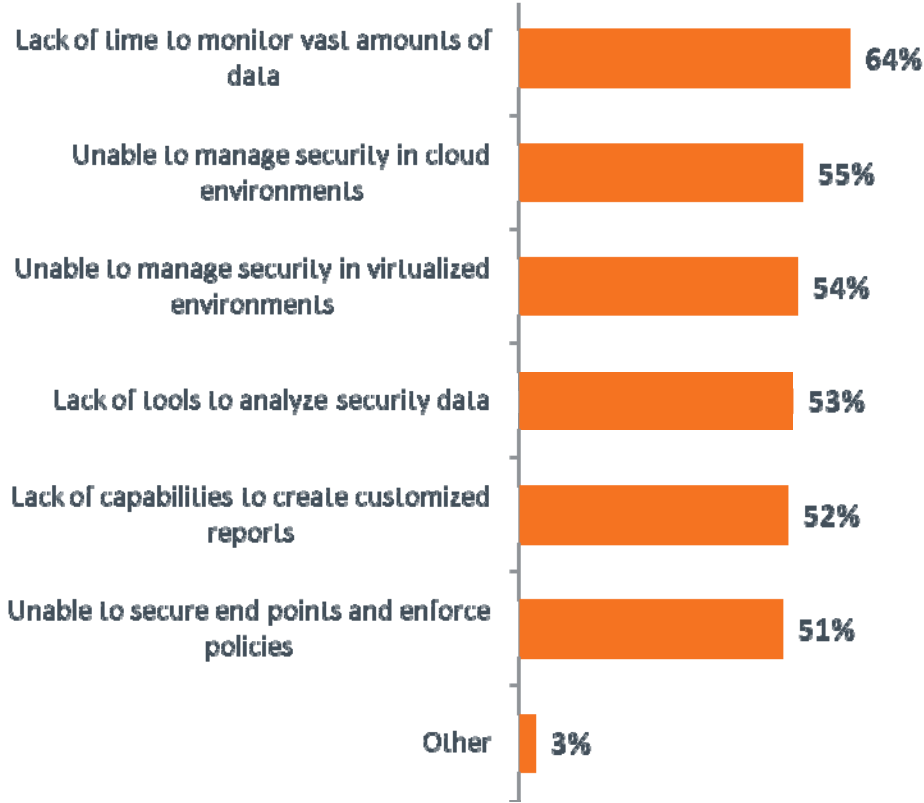
- A percentage that is even higher among very large enterprises (65%) and among those who would classify their organization as “proactive” (63%).

IT security solutions employed today are better than they were five years ago.

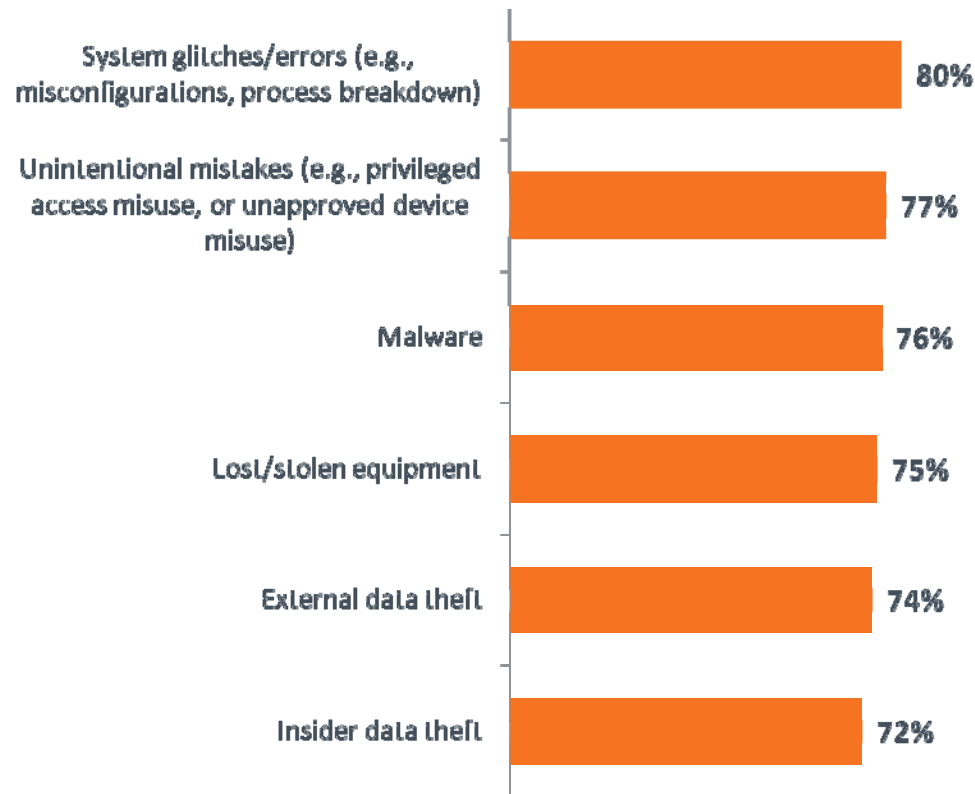
How do your organization's current IT security solutions compare to what your organization used five years ago with regards to reducing risk?



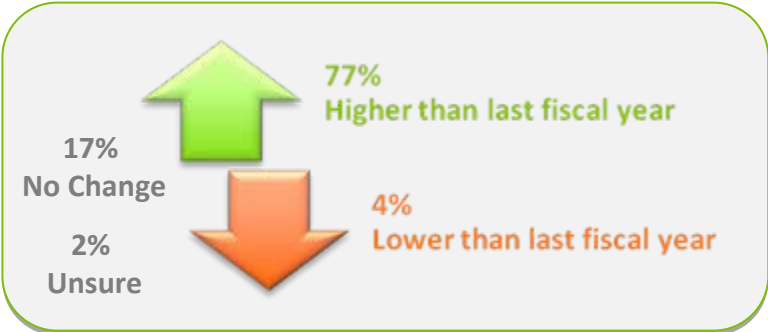
Top challenges organizations face with their current IT security solutions



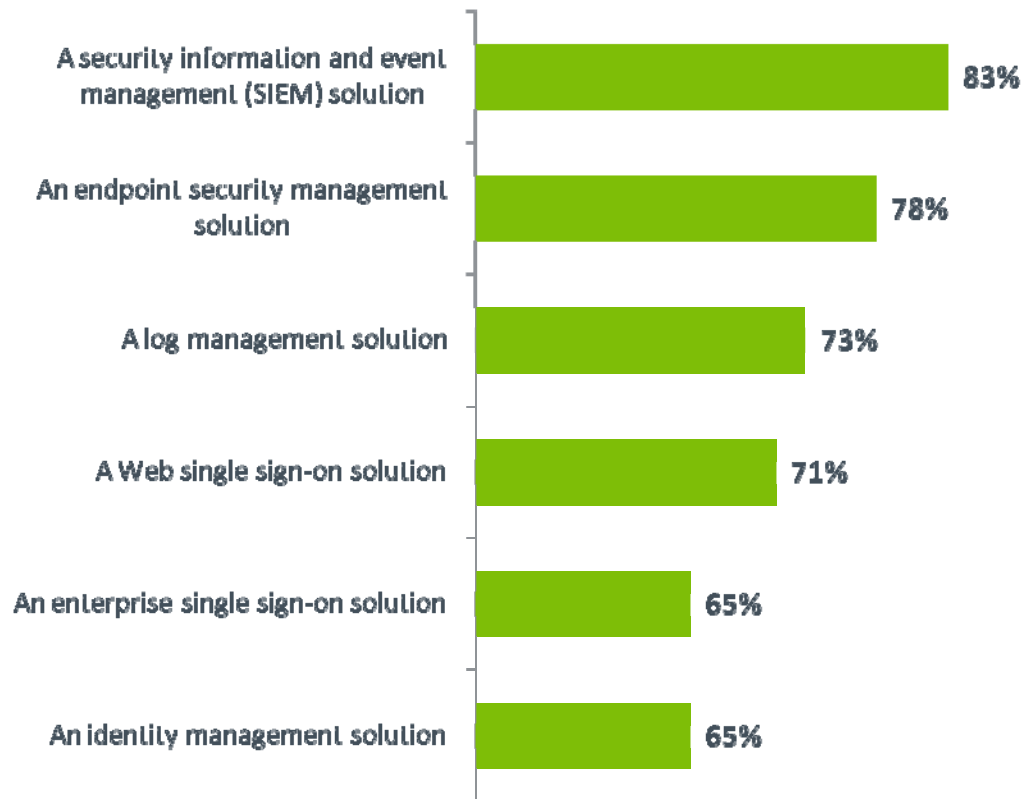
Organizations experienced the following information security breaches in the last two years.



Budgets for IT security solutions over the last fiscal year.



The top IT security solutions organizations are using.



Agreement With Statements About Currently Available IT Security Solutions

